Exhibit D

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

X. Corp.,

Plaintiff,

v.

BRIGHT DATA LTD.

Defendant

Case No. 3:23-CV-03698-WHA

DECLARATION OF RON KOLL IN SUPPORT OF BRIGHT DATA'S PROPOSED PROTECTIVE ORDER

I, Ron Kol, declare under penalty of perjury under the laws of the United States of America as follows:

1. I am Chief Technology and Security Officer for Bright Data Ltd. ("Bright Data"). My responsibilities include overseeing Bright Data's technical infrastructure and the development of technological resources. I am over 18 years of age and have personal knowledge of the facts set forth herein.

2. I am submitting this declaration to explain our concerns if Bright Data's information – including its customer-identifiable information, search-identifiable information, and technical information relating to Bright Data's search-mechanics – were disclosed to X. As I explain below, if this information were disclosed to X, it could cause substantial and irreparable business, commercial, and competitive injury to Bright Data and its customers.

A. Customer-Identifiable Information

3. Customer-identifiable information includes any information from which the identity of the customer could be determined or reasonably inferred. This includes customer names and other customer identifiers, but also includes additional information, such as customer address or search characteristics that may reveal the identity of the customer, either directly or in combination with other documents. Regardless of how the customer's identity is determined, its disclosure to X would cause serious and irreparable harm.

4. Bright Data has developed a relationship and reputation of trust with its customers. That is why some of the most well-known companies and research institutions in the world trust Bright Data to handle their public web data needs. Bright Data does not reveal its customer's identities or use cases without their express consent. Indeed, a critical element of our Master Services Agreement is Bright Data's obligation not to disclose "Confidential Information," which is defined to include, among other things, "customer lists, customer information, [and] end-user information."[1]

5. I understand that X has served discovery requests calling for the identification of Bright Data's customers, including their contracts and communications. I further understand that X wants to give this information to its internal counsel – the very people who, among other things, are tasked with shutting down scrapers (legitimate or not). This would have a devastating effect on Bright Data's business and customer relationships.

6. Disclosure of Bright Data's customers' identities to X's in-house counsel not only threatens to expose these customers to unwarranted and harassing communications, cease-and-desist demands, and subpoenas from X, and threatens Bright Data's customers' reasonable expectations of privacy in their use of Bright Data's services; it also threatens to undo – in an instant – the customer relationship on which Bright Data's business is built.

7. Most of Bright Data's customers are small and do not have the resources to stand up to X. Any communication from X to one of our customers about this case, or about public web scraping generally, inevitably sends a clear message that X (at least) believes the customer is doing something that is either wrongful or that may subject the customer to expensive litigation in the future. This will not only chill legitimate business activity but also cripple Bright Data's business without any ruling as to the merits of this case.

8. There are many other things that X could do to cause harm to Bright Data's customers if it learns their identities. For example, if any of Bright Data's customers have X

[1] https://brightdata.com/license.

accounts or other commercial relationships with X, X could terminate their accounts or relationships, even if there has been no determination that the customers have engaged in any prohibited activity. Bright Data's customers use Bright Data's services for myriad purposes. Such uses include tracking competition, compiling and analyzing public investment data, researching and monitoring marketplace trends, identifying and combating human trafficking, data security testing and monitoring, and more. The vast majority of these uses have ***nothing*** to do with X. And even where customers use Bright Data's services to scrape X, such activities relate solely to logged-off activities. None of this has been judged to be unlawful or in violation of any of X's legal rights.

9. Thus, allowing X or its counsel to even suggest to Bright Data's customers that providing access to public data might be unlawful threatens Bright Data's business beyond what is even at issue in this litigation, and puts a pall over Bright Data's activities before their legality is even determined.

10. X has not provided any case-specific circumstances that would require its in-house counsel to need this information. This shows that discovery in this case may, in fact, be a pretext for obtaining information that can be used in future enforcement actions.

B. Search-Identifiable Information.

11. A central feature of Bright Data's services is that they allow customers to anonymously search public portions of the web. As the Master Services Agreement explains, "Bright Data has developed, owns and offers a service which enables browsing the internet ***anonymously*** by redirecting users' communication through other users' devices." If X obtains information that allows it to de-anonymize the search, it could block future search activity. This would be difficult, if not impossible, for Bright Data to detect, as we would not know why our search failed, and whether it was due to the impermissible use of search-identifiable information produced here in discovery or for some other reason.

12. Bright Data's Master Services Agreement makes clear that search-identifiable information is critical confidential information, which includes as confidential, in part, "all

specifications, formulas, prototypes, computer programs, and … scripts." MSA § 5. This information, for example, would include the customer-specific crawl scripts, the identities of the IP addresses, and proxy servers used in the search.

13. A proxy is an intermediary server, device, or server application that sits between an end-user and a website or other server. There are different types and configurations of proxy servers. When customers use Bright Data's proxy network, Bright Data routes the request from the customer through a third-party device in its proxy network, which then passes the request on to its final destination.

14. Each proxy has its own Internet Protocol address (or "IP address"), which is a numerical label connected to that particular device or proxy. IP addresses identify the source of a particular request and establish a path back to source for the response. Bright Data has built a network with millions of IP addresses geo-located to over 195 countries. Bright Data's IP network is critical to its ability to search and collect public web data because website owners, including X, actively block IP addresses associated with people or entities they do not want to access their public information, whether or not they have any legal right to do so.

15. X has asked for the specific identities of Bright Data's California servers and IP addresses, and it wants to share that information with its anti-scraping team (which includes outside counsel, in-house counsel, and business employees). If X learns the identity of IP addresses in Bright Data's network, it will have the keys to completely shut down Bright Data's access to public information on X's sites, no matter the results of this lawsuit.

16. This is not hypothetical or speculative. X admits in its Complaint that, as part of its efforts to block scraping, it deploys "technological measures," including, among other things, "user identification and IP rate limits."[2] Historically, that strategy has been ineffective against Bright Data precisely because X does not know the specific IP addresses associated with Bright Data's proxy network.

[2] *See* FAC ¶¶ 34-38.

17. X would be able to instantly and irreparably destroy Bright Data's business if it receives a list of these IP addresses. Even if X did not block all of Bright Data's IP addresses, the harm would still be significant and irreparable. If X were to block a single IP address or server, it could not be used for its intended purpose. As such, Bright Data may have to cease using that address or device, stripping it of its intrinsic value to Bright Data. Moreover, Bright Data would have no practical ability to determine if X used search-identifiable information in improper ways. There are many reasons why a particular search may fail to retrieve information, including X's own technological methods to block such searches. It would be impossible to know whether a given search failed because X effectively employed such technologies, or whether X improperly used search-identifiable information it obtained in discovery to block the search.

C. Bright Data's Proprietary Public Web Scraping Technologies.

18. Bright Data is in competition with X. We contend with X every day for access to public data on X's sites. This competition plays out across the queries and responses of the internet. It is a technological arms race to access and view public information.

19. X seeks to block Bright Data's access through various technological means. For example, X deploys CAPTCHAs, user identification protocol, IP rate limiters, and anomaly detection tools to prevent public web searching.[3]

20. While X advertises that it employs these technological measures, it keeps the details hidden and confidential. X seeks to impose a double standard, requiring Bright Data to give X a roadmap to its technology, while keeping its own roadmap secret. Allowing this would fundamentally upset the competitive balance in the marketplace.

21. For its part, Bright Data has developed its own tools that allow it to continue searching for public information despite the technological roadblocks that X installs. One such tool is Bright Data's Web Unlocker. The Web Unlocker is designed to prevent website operators

[3] *See* FAC ¶¶ 34-38.

from blacklisting members of the ***public*** from accessing ***public information*** posted to the Internet.

22. Web Unlocker does this by, for example, rotating the third-party devices that make requests of the website, limiting the number and frequency of requests per IP address, and/or redirecting the search.

23. Just as X keeps the details of its anti-scraping technologies secret, we keep the details of our search technology confidential. Again, our Master Services Agreement makes clear that our Confidential Information includes "all specifications, formulas, prototypes, computer programs and any and all records, data, ideas, methods, techniques, [and] processes" relating to Bright Data's searches.

24. X has asked for every imaginable detail of Bright Data's technologies – from its "development," "testing," "design specifications," "engineering architecture," "service blueprints," down to its very source code. If X were to learn exactly how Bright Data continues to find ways to access and view public information on X's sites, X could shut Bright Data down. It would render Bright Data's years of invested time and resources into its industry-leading technologies moot and useless.

25. If this information were improperly used by X, it would cause irreparable and virtually undetectable harm to Bright Data. As noted above, there are many reasons why a particular search may fail. If information about our search mechanics were disclosed to X, we would be unable to determine whether a failed search was due to X's own technological prowess, or whether it was due to the improper use of discovery materials.

26. In that regard, it is important to note that much of the information X seeks cannot be unlearned by those who receive it. The solutions that Bright Data has developed to combat X's block on public web search can be learned. That information can then be used by X's engineers and coders to develop counter-technologies. In doing so, it would be impossible to determine whether X's engineers and coders came up with creative new solutions, or whether they improperly used Bright Data's confidential information.

D. Bright Data's Proposed Protective Order Significantly Reduces the Likelihood of Substantial Commercial Harm.

27. Bright Data's proposed protective order would protect against the harms of disclosure described above. Bright Data proposes that Highly Confidential Information (including the customer-identifiable information, search-identifiable information, the technical specifics of its technologies) is limited to outside counsel and any experts outside counsel retains. This provides the information to those who need it for purposes of this litigation while keeping it protected from those best positioned to misuse it.

28. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and accurate to the best of my knowledge and belief.

Dated: February 21, 2024

Respectfully submitted,

/s/ Ron Koll
Ron Koll
Chief Technology and Security Officer
BRIGHT DATA LTD.